SYSTEM AND METHOD FOR
DETECTING PURCHASING CARD FRAUD

CROSS-REFERENCE TO RELATED APPLICATIONS

5   This application claims the benefit of U.S. Provisional Application No. 60/105,611, filed on October 26, 1998 and entitled "System and Method For Detecting Credit Card Fraud".

TECHNICAL FIELD

          This invention relates to a system and method for detecting and
10   preventing purchasing card fraud during all phases of a purchasing card life cycle.

BACKGROUND ART

          Roughly half a billion transactions with significant, but preventable, fraud potential occur in the United States each year. Purchasing card contact events that can lead to fraudulent occurrences include application processing, card
15   activation, usage, such as mail and phone ordering, and maintenance events, such as address or other information changes. It is estimated that the total cost of fraud is $1.3 million for every one million gross active accounts, or $1.34 in fraud loss per gross active account (Sources: VISA/MC, Credit Card Prevention Sourcebook).

          A large portion of this fraud could effectively be addressed though
20   improved identification of known fraudulent names, fraudulent addresses, fraudulent phone numbers, fraudulent social security numbers, and other fraudulent personal information. In fact, a large number of fraud cases are typically perpetrated by repeat offenders or organized rings.

          Current tools to combat repeat and organized fraud are still
25   underdeveloped. While there are a myriad of sources for fraud-related information,

the various sources focus on differing pieces of personal data and return fraudulent alerts in non-standard formats. In addition to the lack of uniformity of the alert information, current systems lack real time, "near" real time, or via batch functionality. Furthermore, no single comprehensive source exists that is capable

5   of addressing fraud during the many stages of a purchasing card account.

DISCLOSURE OF INVENTION

Therefore, it is an object of the present invention to provide a system and method for facilitating fraud prevention and detection at all stages of a purchasing card life cycle, wherein purchasing cards are defined as credit cards,

10   debit cards, "Smart" cards (having IC chips), retail cards (such as gas cards), and the like.

It is another object of the present invention to provide a single comprehensive database of standardized fraud data from various contributory sources.

15   It is still another object of the present invention to allow clients to reduce manual processes for fraud detection.

In accordance with these and other objects, the present invention provides a method and system for detecting purchasing card fraud during every aspect of a purchasing card life cycle. A central fraud database is created for

20   receiving known fraudulent or "high risk" personal information. The personal information may include, the fraudulent name, fraudulent addresses, fraudulent phone numbers, fraudulent places of employment, criminal history, and other personal information for example. The central fraud database receives information from a variety of sources including but not limited to proprietary databases, client

25   fraud files, law enforcement, and USPS databases. After a contact event has a occurred the fraud database is scanned for a match between the contact event information and the contents of the fraud database. If a possible fraud match occurs

the system sends a fraud alert to the client or user of the database. The present invention has many advantages over the prior art for example the present invention has the capability to send fraud alerts in real time, "near" real time, or via batch to clients thus reducing or eliminating the damage caused by potential purchasing card fraud.

Thus in accordance with one aspect of the present invention, a method is provided for detecting purchasing card fraud during all phases of a purchasing card life cycle. The method includes obtaining contact event information from a client during a contact event, comparing the contact event information with information stored in a database, and sending a fraud alert to a client in real time, "near" real time, or via batch for communicating to the client that a potential fraud match has occurred. Thus the method allows for special handling of the contact event by the client or user of the database.

In accordance with another aspect of the present invention, a system for detecting purchasing card fraud during all phases of a purchasing card life cycle is provided. The system has a computer database for receiving contact event information from a client, computer software in communication with the computer database for comparing the contact event information with information stored in the database, and a communication network for sending a fraud alert to a client in real time, "near" real time, or via batch for informing the client that a potential fraud match has occurred.

The above objects and other objects, features, and advantages of the present invention are readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying drawings.

BRIEF DESCRIPTION OF DRAWINGS

FIGURE 1 is a schematic representation of a purchasing card fraud detection system designed in accordance with the present invention;

5   FIGURE 2 is a flow diagram of a preferred method of detecting purchasing card fraud in accordance with the present invention;

FIGURE 3 is a flow diagram of a preferred fraud matching process; and

FIGURE 4 is a schematic representation of a preferred fraud database architecture.

10   ## BEST MODE FOR CARRYING OUT THE INVENTION

The present invention provides a system and method for facilitating fraud prevention and detection for all contact events during a purchasing card life cycle. Such contact events include 1) application processing; 2) card activation; 3) cardholder usage, including mail and telephone orders; and 4) maintenance events,

15   such as name and address changes, PIN changes, plastic requests, and credit line increases.

With reference to FIG. 1, the system of the present invention preferably includes a single, comprehensive risk database 10 for the detection of purchasing card fraud. The risk database 10 may include information from various

20   sources 12, as will be described below. The risk database is preferably server-based and has connectivity, via a local area network 14 (LAN) or other network, to a mainframe 16. The mainframe 16 is provided for on-line transactions involving the various contact events 18 described above. Clients 20 are provided with connectivity to the risk database 10 for file transfer and general access, and are also provided

25   connectivity to mainframe 16 (Graphical User Interface, dummy terminal or the like)

for receipt of fraud alerts and queue information. An optional, more limited database (not shown) could be provided for non-contributors to the risk database. Preferably, a backup server is provided.

The system of the present invention possesses the technical functionality to pool data from multiple sources in multiple formats and to standardize reporting structure guidelines, enabling the risk database to function for many types of transactions or contact events 18. In addition, the system provides the ability to query in real time, "near" real time, or via batch with on-line interfaces to the mainframe transactions. Preferably, limited client 20 resources are required for access.

In a preferred embodiment, at the mainframe 16 level, a daily queue statistics report is developed at the client 20 level to identify all accounts that match the risk database 10, including the source of the data match. Furthermore, at the server level, reports are generated which track contributor statistics. In addition, reporting is developed to track client statistics on a query basis, such as by the number of record transactions queried against the risk database 10, or by the number of records with a data match.

Possible sources for the consortium fraud database 10 include client databases, credit card issuer databases, credit bureau databases, research and investigation fraud files, ANI risk databases, the U.S. Postal Service NRI database, Account Takeover modeling/scoring, the Social Security Administration, the Department of Motor Vehicles, Western Union, Telecheck, the American Business List, law enforcement, court and public information records, phone directories, and direct mail surveys.

From such sources, the available data includes, but is not limited to, 1) personal information, such as addresses, phone numbers, and social security numbers used in known frauds; 2) valid US addresses and their nature, i.e. residential, commercial, or vacant; 3) valid address/name combinations; 4) high risk

zip codes; 5) public information, such as bankruptcy filings, tax liens, and civil judgments; and 6) consumer and purchase data.

The proposed data element structure within the risk database preferably includes at least the following:

5   1.   Names of fraudulent or potentially fraudulent ("high risk") primary, secondary, and additional cardholders in the form of first name, last name, and middle initial.

2.   Fraudulent or potentially fraudulent ("high risk") home and business addresses, including P.O. Box, city, state, and zip code.

10   3.   Fraudulent or potentially fraudulent ("high risk") home and business telephone numbers.

4.   Fraudulent or potentially fraudulent ("high risk") social security numbers of primary, secondary, and additional cardholders.

The risk database would act as a central repository for fraud data to

15   be queried against by lenders and adjacent market users. Potential primary users or clients include bank card issuers, non-bank card issuers, potential card issuers, oil card issuers, merchants, and retailers. Possible secondary users include phone companies, DDA Account banks, and utility companies, among others.

The method of detecting potential purchasing card fraud of the present

20   invention is outlined in the flow diagram of FIG. 2. The method includes obtaining contact event information at the mainframe 16, as represented by block 50. Comparing the contact event 18 information to fraud information stored in the risk database 10, as represented by block 52. If a match is found between the contact event information and the fraud information, the method further includes issuing an

25   on-line alert to the client and queuing the information for manual review by the particular client, as represented by block 54. If a match does not occur client 20 is notified as such and communication with risk database 10 is concluded, as represented by block 56. Optionally, a fraud match may be scored, as represented by block 58 and as will be explained below. If a client 20 does not wish to receive

30   a score then communication with the database is concluded, as represented by block

60. However, if a client has elected to receive a match score, a scorecard is generated and sent to the client 20, as represented by block 62 and then communication with risk database is terminated at block 64.

Within the system of the present invention, contact event 18 transactions are preferably structured to create automatic queries which compare account record data elements against the fraud information stored in the risk database. If a match is found between the account data and the fraud data, then an alert message is generated by the system in real time, "near" real time, or via batch to the queue. In addition, the account record is sent to an on-line queue to be monitored and/or manually worked by the client. Upon entry to the queue, the contact event transaction is suspended or placed on hold until manual follow-up is completed. The contact event information may for example be purged from the database.

An additional feature of the present invention is to offer clients 18 the option of having matched fraud data records "scored" to assist in the decisioning/actioning processes when a record is queued. Preferably, a generic suite of scorecards is provided, while also allowing client-defined scorecards to be developed and implemented. In a preferred embodiment, a scorecard is provided which predicts the likelihood of a fraudulent takeover of an existing, active, or inactive cardholder account.

The following attributes of the invention are thus possibly provided to facilitate fraud detection at all stages of a purchasing card life cycle:
- Application Processing
- Card Activation
- Cardholder Usage/Maintenance
- Other Transaction or Contact Events: Priority Non-Mons: PIN changes, plastic requests, credit line increases and changes to the account record.

The components of the invention are:

- Consortium Data Warehouse
- Fraud Scoring
- Actioning (Alerts to On-Line Screens)

5

- Queuing for Manual Review

The Matching Process

As shown in Figure 3, selected non-monetary transactions may be structured to create queries which compare account record data elements against the Consortium Risk Database 10 of the invention. For example, during an account

10   entry transaction 80 (application processing, card activation, mail/phone order, address change, and the like) could automatically compare key application data elements against the Data Warehouse or Risk Database 10. If a match is found, as represented by block 82, between the account and the Data Warehouse, then an alert message 84 would be generated by the system real time, "near" real time, or via

15   batch. In addition, the account record may be sent to an on-line queue 86 to be monitored and/or manually worked by the client. Upon entry to the queue, the non-monetary transactions would be suspended or placed on hold until manual follow up is completed. In the case of new account entries and batch-entered new accounts, the accounts may be built on the system, however, plastic generation would be

20   suspended.

Information residing within the queue would include the account record information, the reason for the alert (i.e., potential fraudulent name, address, SSN, or phone number), and the contributing source of the matched data. This process will help to reduce responsibility/liability for data integrity.

25   Scoring of Matched Data

In further keeping with the invention, clients will be provided the option of having matched fraud data records "scored" to assist in the decisioning/actioning processes when a record is queued, as represented by block 88. This should provide business opportunities to build the appropriate scorecard logic.

-8-

Accordingly, a generic suite of scorecards 90 may be implemented as well as client-defined scorecards 92.

Consortium Contributors

5   All consortium contributors will be allowed access to the entire data warehouse. Usage incentives may also be provided for "global" contributors. An example of a usage incentive may be reduced fees for accessing the fraud database. Other incentives may include partial to full access to information contained in the fraud database.

10   ## Non-Consortium User

A non-contributor to the consortium may be offered access to information that the database manager may have purchased or provided in a non-consortium database 100. Otherwise non-contributors may be restricted from information provided by "global" contributors to the Risk Consortium Database.

15   ## Summary of Benefits and Critical Needs Met

- Provides a single source of uniform data from various contributor business sources;
- Increases the effectiveness of fraud detection efforts;
- Allows clients to reduce current manual processes for fraud
20   identification and actioning;
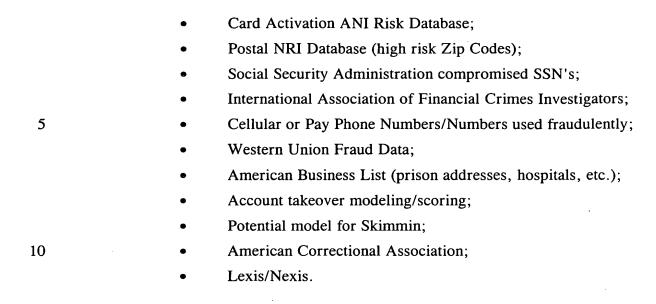- Pools data across the client base to improve identification of repeat offenders.

Consortium Risk Data Warehouse

A consortium data warehouse contains data contributed from various
25   business sources 110 including, but not limited to:

- Clients;
- Research and Investigation Fraud Files (Fraud App's and Account takeovers (type lost 3,5,8));
- Customer Service Fraud File Database;

- Card Activation ANI Risk Database;
- Postal NRI Database (high risk Zip Codes);
- Social Security Administration compromised SSN's;
- International Association of Financial Crimes Investigators;

5

- Cellular or Pay Phone Numbers/Numbers used fraudulently;
- Western Union Fraud Data;
- American Business List (prison addresses, hospitals, etc.);
- Account takeover modeling/scoring;
- Potential model for Skimmin;

10

- American Correctional Association;
- Lexis/Nexis.

Proposed Data Element Structure

As depicted in Figure 4, the data element structure 200 may include:

15

- Name (Primary and Secondary and additional): First, Last, Middle Initial;
- Address: Home, Business (including PO Box);
- City;
- State;

20

- Zip Code;
- Phone: Home, Business;
- Social Security Number: Primary, Secondary;
- High Risk Zip Codes (NRI data); and
- Known fraudulent accounts determined by type lost.

25   Therefore, the system and method of the present invention provide a single source of uniform data from various contributor business sources 210, increase the effectiveness of fraud detection efforts, allow clients 212 to reduce current manual processes for fraud identification and actioning, and allow pooling of data across the client base to improve the identification of repeat offenders.

While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes

5 may be made without departing from the spirit and scope of the invention.